us. Deportment
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: EQUIPMENT, SYSTEMS, AND INSTALLATIONS IN PART 23 AIRPLANES

Date: 3/12/99
Initiated By: ACE-100

AC No: 23.1309-1C
Change:

1. PURPOSE. This advisory circular (AC) provides guidance and information for an acceptable means, but not the only means, for showing compliance with the requirements of § 23.1309(a) and (b) (Amendment 23-49) for equipment, systems, and installations in Title 14 Code of Federal Regulations (14 CFR) Part 23 airplanes. This material is neither mandatory nor regulatory in nature and does not constitute a regulation.

a. Broad Causes of Fatal Accidents:

(1) The primary objective of this revision to the AC is to improve the safety of the airplane fleet by fostering the incorporation of both new technologies that address pilot error and weather related accidents and those technologies that can be certificated affordably under 14 CFR Part 23. Pilot error accidents, the largest single cause, often are the result of a lack of situational awareness relative to terrain or weather, or to a loss of control due to excess workload. Incorporating technologies that exceed the capability and reliability of the systems found in the current fleet, which primarily have a certification basis prior to Amendment 23-4 1, should improve safety. This strategy is in concert with the Federal Aviation Administration's (FAA) safety objective to reduce accidents.

(2) Accident rate is a function of many factors, which include human performance, weather, design, operation, training, maintenance, and airspace system infrastructure. For all airplanes, but particularly General Aviation (GA) airplanes, pilot error causes most accidents. Correct pilot interventions and actions could prevent some of these accidents. A reduction in the frequency or the severity of the effects of errors has the greatest potential for improving aviation safety. An increase in avionics equipage rates and improved pilot situational awareness should have a significant positive impact on the GA accident rate.

b. *Installing Affordable Systems:*

(1) Enhancing the quantity, quality, and presentation of situational data available to the pilot in the cockpit can improve pilot situational awareness. Many studies have shown that equipping

these airplanes with safety devices such as Terrain Awareness Warning Systems and Advanced Weather Display Systems may dramatically reduce a number of accident types. For GA airplanes, the cost of such devices currently is prohibitive. The cost of certifying these systems in airplanes is an added layer to the recurring cost per part and per installation. Lower equipage rates associated with increased costs impede safety benefits.

(2) Appropriate human factors in the design, operation, and use of systems and equipment may contribute to enhancing safety. The safety improvements from the widespread use of this equipment should be much greater than the accidents that might result from failure or malfunction of the equipment. This improvement should occur even if an increase in the number of equipment failures results from a relaxation of the existing certification standards.

(3) The certification standards being changed were incorporated by using the standards developed for transport airplanes. Incorporation of these standards into Part 23 resulted in a significant increase in equipment reliability standards. That is, they required much lower probability values for failure conditions than the existing operational safety history of different airplane classes. Current data indicates that these probability values were not realistic. Since most aircraft accidents are caused by something other than equipment failures, increasing the reliability of the installed systems to try to improve safety will have little positive effect on reducing aircraft accidents when compared with reducing accidents due to pilot error. If systems are required to meet safety and reliability parameters much greater than the operational environment, the cost of the improved systems are driven to a level that makes them impractical. The aviation industry as a whole is on the threshold of a revolutionary change in communication, navigation, and surveillance of aircraft operations. This complete overhaul of the National Airspace System (NAS) is intended to take advantage of new technology and will likely result in the long-term replacement of nearly all avionics and instrument equipment in the existing fleet as well as in new production aircraft. If general aviation is to operate within a revised NAS system, new technologies must be available and affordable for GA aircraft. Under the existing certification process, new technologies such as digital communications, data buses, satellite-based navigation, and data links would be unaffordable for GA. This situation would result in either incomplete NAS architecture implementation or exclusion of large portions of the GA fleet from the NAS system. Neither situation is desirable or acceptable.

(4) This AC is revised to facilitate the introduction of safety enhancing new technologies for GA airplanes. Overall, facilitating the installation of safety equipment may enhance NAS safety. A multi-tiered certification with different criteria for probability of failure and software development assurance may be acceptable for systems and for enhancing equipment on GA airplanes. Probability of failures and Software Assurance Development Levels that are different from the criteria applicable to transport airplanes are justified.

2. CANCELLATION. AC 23.1309-1B, Equipment, Systems, and Installations in Part 23 Airplanes, dated July 28, 1995, is canceled.

3. BELATED REGULATIONS AND DOCUMENTS.

a. ***Regulations:*** Sections 23.1301 and 23.1309 of Part 23 (through Amendment 23-49).

b. ***Advisory Circulars and Notices:*** Obtain the AC's listed below from the U.S. Department of Transportation, Subsequent Distribution Office, Ardmore East Business Center, 3341 Q 75th Avenue, Landover, MD 20785 :

AC 20-53A	Protection of Aircraft Fuel Systems Against Fuel Vapor Ignition Due to Lightning
AC 20-l 15B	RTCA, Inc., Document RTCA/DO-178B
AC 20-136	Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning
AC 21-16D	RTCA/DO160D
AC 23-15	Small Airplane Certification Compliance Program
AC 23.1311-1A	Installation of Electronic Displays in Part 23 Airplanes
AC 23.1329-2	Automatic Pilot System Installation in Part 23 Airplanes
AC 25.1309-1A	System Design and Analysis

c. Industry Documents:

(1) Obtain the RTCA documents listed below from the RTCA, Inc., 1140 Connecticut Avenue, NW, Suite 1020, Washington, D.C. 20036-4001:

RTCA/DO-160D	Environmental Conditions and Test Procedures for Airborne Equipment
RTCA/DO-178A/B	Software Considerations in Airborne Systems and Equipment Certification

(2) Obtain the SAE documents listed below from the Society of Automotive Engineers, Inc., 400 Commonwealth Drive, Warrendale, PA 15096-000 1:

ARP 926A/B	Fault/Failure Analysis Procedure
ARP 1834/A	Fault/Failure Analysis for Digital Systems and Equipment
ARP 4754	Certification Considerations for Highly Integrated or Complex Aircraft Systems
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Note: Historically, Aerospace Recommended Practices (ARP's) 926A and 1834 provided appropriate guidance for safety assessment of Part 23 airplanes. ARP's 926B and 1834A revised ARP's 926A and 1834, respectively. The scope sections of ARP's 926B and 1834A state that ARP 4761 provides updated methods and processes for use on civil aircraft safety assessments. When performing civil aircraft safety assessments, ARP-4761 should be used in lieu of ARP's 926B or 1834A. If ARP's 926B or 1834A are used, specific processes addressed in ARP 4761, but not in ARP's 926B or 1834A, should be considered.

ARP's 4754 and 4761 state that these documents describe guidelines and methods of performing the safety assessment for certification of civil aircraft. They further state that the guidance material in these ARP's were developed in the context of 14 CFR Part 25 and the Joint Aviation Requirements 25 (JAR 25). They are primarily associated with showing compliance with Part 25, § 25.1309/JAR 25.1309. A subset of this material may be applicable to non-25.1309 equipment, such as other requirements in Parts 23, 25, 27, 29, and 33. However, some of the processes included are not necessary or appropriate for Part 23 airplanes. ARP 4754 contains tutorial information on applying specific engineering methods that an applicant may wish to utilize in whole or in part.

This AC is not intended to constrain the applicant to the use of these documents in the definition of their particular methods of satisfying the objectives of this AC. However, these documents contain material and methods of performing the System Safety Assessment that an applicant may choose to use.

d. ***Related Reading Material:*** A comprehensive discussion of lightning protection, with additional nonregulatory guidance information, is available in the current edition of FAA Report DOT/FAA/CT-89/22, "Aircraft Lightning Protection Handbook," dated September 1989. This document is available to the public through the National Technical Information Service, Springfield, VA 22161.

4. APPLICABILITY.

a. This AC is generally applicable only to the original applicant seeking issuance of a type certificate (TC), amended type certificate (ATC), and supplemental type certificate (STC) for the initial approval of the new type design or a change in the type design. This document addresses general applicability, and it should not be utilized to replace any specific guidance intended for individual types of equipment, systems, and installations. Because § 23.1309 is a regulation of general requirements, it should not be used to supersede any specific requirements of Part 23. However, since software is not addressed elsewhere in Part 23, the software development assurance criteria of this AC are applicable. For example, § 23.13 11, Electronic display instrument systems, has specific requirements on the number of electronic displays required for attitude, airspeed, and altitude; therefore, $23.1309 should not be used to increase or decrease the requirements (except for determining the Software Development Assurance Level). For either mechanical or analog electromechanical systems, or both, where the installation is not complex, the single-fault concept and experience that are based on service-proven designs and engineering judgment are appropriate. In this case, a Functional Hazard Assessment (FHA), a design appraisal, and an installation appraisal, in accordance with Item 9.d.(6), may satisfy § 23.1309(b).

b. Section 23.1309 does not apply to the performance, flight characteristics, and structural loads and strength requirements of Subparts C and D, but it does apply to any system on which compliance with the requirements of Subparts B, C, and D is based. For example, it does not apply to an airplane's inherent stall characteristics or their evaluation of § 23.201, but it does apply to a stick pusher (stall barrier) system installed to attain compliance with § 23.20 1.

c. Section 23.1309 is applicable to the installation of all airplane systems and equipment, which includes pneumatic systems, fluid systems, electrical/electronic systems, mechanical systems, and power-plant systems included in the airplane design, except for the following:

(1) Systems and installations approved only as part of a type-certificated engine or propeller, and

(2) The flight structure (such as wings, fuselage, empennage, control surfaces, mechanical flight control cables, pushrods, control horns, engine mounts, and structural elements of the landing gear) requirements are specified in Subparts C and D of Part 23.

5. BACKGROUND.

a. Amendment 23-14 adopted the original airworthiness standards in § 23.1309(a). Prior to Amendment 23-14 to Part 23 (effective December 20, 1973), neither Part 3 of the Civil Air Regulations (CAR) nor 14 CFR Part 23 contained safety requirements in § 23.1309 for equipment, systems, and installations for small airplanes. In 1968, the FAA instituted an extensive review of the airworthiness standards of Part 23. Because of the increased use of Part 23 airplanes in all weather operations and the pilot's increased reliance on installed systems and equipment, the FAA promulgated $23.1309 to provide for an acceptable level of safety for such equipment, systems, and installations. When the FAA adopted $23.1309 (Amendment 23-14), it did not envision that systems that perform critical functions would be installed in small airplanes; therefore, prior to Amendment 23-41, this section did not contain safety standards for evaluating critical functions. When such equipment, systems, and installations were included in the airplane design, they were evaluated under special conditions in accordance with the procedures of 14 CFR Part 2 1.

b. With the adoption of Amendment 23-34 (effective February 17, 1987), § 23.1309 was expanded to include certification of commuter category airplanes. This expansion added a requirement to ensure that applicable systems and installations are designed to safeguard against hazards. It also added requirements for equipment identified as essential loads and the affected power sources.

c. With the adoption of Amendment 23-41 (effective November 26, 1990), § 23.1309 retained the existing safety requirements adopted by Amendment 23-14 for airplane equipment, systems, and installations that are not complex and that do not perform critical functions. For those cases where the applicant finds it necessary or desirable to include complex systems, or systems that perform critical functions, Amendment 23-4 1, § 23.1309, provides additional requirements for identifying such equipment, systems, and installations. It also provides additional requirements needed for certification. This amendment permitted the approval of more advanced systems having the capability to perform critical functions.

d. With the adoption of Amendment 23-49 (effective March 11, 1996), § 23.1309(a)(4) was amended to correct the error in Amendment 23-42, which inadvertently removed the commuter category requirement. Amendment 23-34 originally added the commuter category requirements of § 23.1309(a)(4) to Part 23 as § 23.1309(d), but the requirements were inadvertently not incorporated into § 23.1309 as adopted by Amendment 23-41. Amendment 23-49 corrected this error by again adding the requirements to Part 23 as § 23.1309(a)(4).

e. Qualitative and quantitative analyses are often used in assessing the acceptability of complex designs that have a high degree of integration, that use new technology, that are new or different applications of conventional technology, or are designs that perform critical functions. These assessments lead to the selective use of quantitative analyses both to support experienced engineering and operational judgment and to supplement qualitative analyses and tests. Numerical probability ranges, associated with the terms used in § 23,1309(b), are accepted for evaluating quantitative analyses that have a logical and acceptable inverse relationship between the probability and severity of each Failure Condition.

6. DEFINITIONS.

a. ***Adverse Effects:*** A response of a system that results in an undesirable operation of an airplane system, or subsystem.

b. ***Analysis and Assessment:*** The terms "analysis" and "assessment" are used throughout, Each has a broad definition and the two terms are, to some extent, interchangeable. However, the term "analysis" generally implies a more specific and more detailed evaluation, while the term "assessment" may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application (for example, Fault Tree Analysis (FTA), Markov Analysis, Preliminary System Safety Assessment (PSSA), etc.).

c. Adverse Operating Condition: A set of environmental or operational circumstances applicable to the airplane, combined with a failure or other emergency situation that results in a significant increase in normal flight crew workload.

d. ***Attribute:*** A feature, characteristic, or aspect of a system or a device, or a condition affecting its operation. Some examples would include design, construction, technology, installation, functions, applications, operational uses, and environmental and operational stresses. It would also include relationships with other systems, functions, and flight or structural characteristics.

e. Average Probability Per Flight Hour: This term is defined for this AC as a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all airplanes of a type divided by the anticipated total operating hours of all airplanes of that type. (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration.) See Appendix C.

f. ***Complex:*** A system is "Complex" when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods. Failure Modes and Effects Analysis (FMEA) and FTA are examples of such methods.

g. Continued Safe Flight and Landing: This phrase means that the airplane is capable of continued controlled flight and landing, possibly using emergency procedures, without requiring exceptional pilot skill or strength. Upon landing, some airplane damage may occur as a result of a Failure Condition.

h. ***Conventional:*** A system is considered "Conventional" if its function, the technological means to implement its function, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used. The systems that have established an adequate service history and the means of compliance for approval are generally accepted as "Conventional. "

i. ***Critical Function:*** A function whose loss would prevent the continued safe flight and landing of the airplane. *Note:* The term "Critical Function" is associated with a Catastrophic Failure Condition. Newer documents may not refer specifically to the term "Critical Function."

j. Design Appraisal: A qualitative appraisal of the integrity and safety of the system design, such as the effective use of design techniques to verify that failures of a system do not adversely affect other systems. An effective appraisal requires experienced judgment.

k. ***Development Assurance:*** All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.

1. Equipment Essential to Safe Operation: Equipment installed in order to comply with the applicable certification requirements of Part 23 or operational requirements of Parts 91 and 135.

m. ***Error:*** An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.

n. ***Essential Function:*** A function whose loss would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. *Note:* The term "Essential Function" is associated with Failure Conditions between Major and Hazardous. Newer documents may not refer specifically to the term "Essential Function."

o. Event: An occurrence that has its origin distinct from the airplane, such as atmospheric conditions (for example, gusts, temperature variations, icing, and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

p. ***Essential Load:*** Equipment essential to safe operation that requires a power source for normal operation.

q. ***Extremely Remote Failure Conditions:*** Those Failure Conditions not anticipated to occur to each airplane during its total life but which may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for Hazardous Failure Conditions in Figure 2.

r. ***Extremely Improbable Failure Conditions:*** For commuter category airplanes, those Failure Conditions so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type. For other classes of airplanes, the likelihood of occurrence may be greater. For quantitative assessments, refer to the probability values shown for Catastrophic Failure Conditions in Figure 2.

s. Failure: An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). *Note:* Errors may cause failures but are not considered failures.

t. ***Failure Conditions:*** A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events. Failure Conditions may be classified according to their severity as follows:

(1) No ***Safety Effect:*** Failure Conditions that would have no affect on safety (that is, Failure Conditions that would not affect the operational capability of the airplane or increase crew workload).

(2) Minor: Failure Conditions that would not significantly reduce airplane safety and involve crew actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in crew workload (such as routine flight plan changes), or some physical discomfort to passengers or cabin crew.

(3) Major: Failure Conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins or functional capabilities; a significant increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.

(4) Hazardous: Failure Conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following:

(i) A large reduction in safety margins or functional capabilities;

(ii) Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or

(iii) Serious or fatal injury to an occupant other than the flight crew.

(5) Catastrophic: Failure Conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane. *Notes:* (1) The phrase "are expected to result" is not intended to require 100 percent certainty that the effects will *always* be catastrophic, Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic, (2) The term "Catastrophic" was defined in previous versions of the rule and the advisory material as a Failure Condition that would prevent continued safe flight and landing.

u. ***Function:*** The lowest defined level of a specific action of a system, equipment, and flight crew performance aboard the airplane that, by itself, provides a complete recognizable operational capability (for example, an airplane heading is a function). One or more systems may contain a specific function or one system may contain multiple functions.

v. Functional Hazard Assessment: A systematic, comprehensive examination of airplane and system functions to identify potential Minor, Major, Hazardous, and Catastrophic Failure Conditions that may arise as a result of a malfunction or a failure to function.

w. Hazard: Any condition that compromises the overall safety of the airplane or that significantly reduces the ability of the flight crew to cope with adverse operating conditions.

x. Improbable Failure Conditions: Those Failure Conditions unlikely to occur in each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type. Also, those Failure Conditions not anticipated to occur to each airplane during its total life but that may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for Major and Hazardous Failure Conditions in Figure 2. For more specific guidance, see definitions of "Remote Failure Conditions" and "Extremely Remote Failure Conditions."

y. Installation Appraisal: A qualitative appraisal of the integrity and safety of the installation. Any deviations from normal industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications that are made after entry into service.

z. Latent Failure: A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one that would, in combination with one or more specific failures or events, result in a Hazardous or Catastrophic Failure Condition.

aa. ***Malfunction:*** Failure of a system, subsystem, unit, or part to operate in the normal or usual manner. The occurrence of a condition whereby the operation is outside specified limits.

bb. ***Minimize:*** To reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. The least practical amount is that point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction. Additional efforts would not result in any significant improvements to safety and would inappropriately add to the cost of the product without a commensurate benefit.

cc. ***Power Source;*** A system that provides power to installed equipment. This system would normally include prime mover(s), required power converter(s), energy storage device(s), and required control and interconnection means.

dd. ***Probable Failure Conditions:*** Those Failure Conditions anticipated to occur one or more times during the entire operational life of each airplane. These Failure Conditions may be determined on the basis of past service experience with similar components in comparable airplane applications.

ee. Primary Function: A function that is installed to comply with the applicable regulations for the required function and that provides the most pertinent controls or information instantly and directly to the pilot.

ff. Qualitative: Those analytical processes that assess system and airplane safety in an objective non-numerical manner.

gg. Quantitative: Those analytical processes that apply mathematical methods to assess the system and airplane safety.

hh. ***Redundancy:*** The presence of more than one independent means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical.

ii. ***Reliability:*** The determination that a system, subsystem, unit, or part will perform its intended function for a specified interval under certain operational and environmental conditions.

jj. Remote Failure Conditions: Those Failure Conditions that are unlikely to occur to each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type. For quantitative assessments, refer to the probability values shown for Major Failure Conditions in Figure 2.

kk. ***Similarity:*** The process of showing that the equipment type, form, function, design, and installation is nearly identical to already approved equipment. The safety and operational characteristics and other qualities should have no appreciable affects on the airworthiness of the installation.

II. Single Failure Concept. The objective of this design concept is to permit the airplane to continue safe flight and landing after any single failure. Protection from multiple malfunctions or failures should be provided when the first malfunction or failures would not be detected during normal operations of the airplane, which includes preflight checks, or if the first malfunction or failure would inevitably cause other malfunctions or failures.

mm. ***System:*** A combination of components, parts, and elements that are interconnected to perform one or more functions.

nn. ***Warning:*** A clear and unambiguous indication to the flight crew or pilot of a failure that requires immediate corrective action. An inherent characteristic of the airplane or a device that will give clearly distinguishable indications of malfunction or misleading information may provide this

warning. Note: The requirements of §§ 23.1309(b)(3) and 23.1322 are incompatible. Until such time as a rule change can resolve this discrepancy, if immediate crew recognition and corrective or compensatory action by the crew is required, a warning must be provided. If immediate crew awareness is required and subsequent crew action will be required, a caution should be provided.

7. APPLICATION OF § 23.1309(a), (a)(l), (a)(2), AND (a)(3), AS ADOPTED BY AMENDMENTS 23-41 AND 23-49.

a. If the certification basis for the airplane is Amendment 23-14, § 23.1309(a) (See *NOTE)* is appropriate to use for systems in airplanes approved to fly either Visual Flight Rules (VFR) or Instrument Flight Rules (IFR), or both. Systems that meet the single-fault concept comply with the requirements of § 23.1309(a). Compliance with § 23.1309(b) is not required and a safety assessment is not necessary, but it may be used. For complex systems, the requirements of Amendment 23-14 may not provide an adequate level of safety.

NOTE: All references to regulatory sections in this paragraph refer to § 23.1309, as amended by Amendment 23-49. The requirements of paragraphs (a), (a)(l), (a)(2), and (a)(3) of § 23.1309, as amended by Amendments 23-41 and 23-49, are the same requirements in paragraphs (a), (b), and (c) of § 23.1309, as amended by Amendment 23-14.

b. Experienced engineering and operational judgment should be applied when determining whether or not a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems attributes should be considered; however, the complexity of the software and hardware need not be a dominant factor in the determination of the need to conduct a system safety assessment. For example, the design may be complex, such as a satellite communication system used only by the passenger, but its failure may cause only minor safety effects.

c. In order to show compliance with the requirements of § 23.1309(a), (a)(l), (a)(2), and (a)(3), it will be necessary to verify that the installed systems and equipment will cause no unacceptable adverse effects and to verify that the airplane is adequately protected against any hazards that could result from probable malfunctions or failures. A probable malfunction or failure is any single malfunction or failure that is considered probable on the basis of either past service experience or analysis with similar components in comparable airplane applications, or both. Multiple malfunctions or failures should be considered probable if either the first malfunction or failure would not be detected during normal operation of the system, which includes preflight checks, or if the first malfunction or failure would inevitably lead to other malfunctions or failures. Analyze, inspect, and test equipment, systems, and installations to ensure compliance with the requirements of § 23.1309(a), (a)(l), (a)(2), and (a)(3). A step-by-step diagram to comply with § 23.1309(a), (a)(1), (a)(2), and (a)(3) is shown in Figure 1, and these steps are listed below.

(1) Evaluate all airplane systems and equipment in order to determine whether they are the following:

(i) Essential to safe operation; or

(ii) Not essential to safe operation,

(2) Determine that operation of installed equipment has no unacceptable adverse effects. Verify this by applicable flight or ground checks, as follows:

(i) If it can be determined that the operation of the installed equipment will not adversely affect equipment essential to safe operation, the requirements of § 23.1309(a)(l)(i) have been satisfied; and

(ii) If it is determined that the operation of the installed equipment has an adverse affect on equipment not essential to safe operation and a means exists to inform the pilot of the effect, the requirements of § 23.1309(a)(l)(ii) have been met. An acceptable means to inform the pilot that the affected system is not performing properly would include any visual or aural method (flags, lights, horns, loss of display, etc.).

(3) Determine that failure or malfunction of the installed equipment could not result in unacceptable hazards.

(i) All equipment should be evaluated for general installation hazards. These types of hazards would normally include those hazards that would directly compromise the safety of the airplane or its occupants, such as fire, smoke, explosion, toxic gases, depressurization, etc. A hazard could also result from loss of equipment or systems essential to safe operations when the minimum required functions are lost. Individual failure of redundant equipment would not necessarily be considered a hazard. For example, the single failure of either a communication transceiver or a navigation receiver (but not both) during IFR operation is not considered a hazard; however, a single failure of a common power supply to those systems would be considered a hazard.

(ii) Systems and equipment essential to safe operation should also be assessed for probability of malfunction or failure if loss of required functions could result in a hazard. Where the installation is conventional, and where there is a high degree of similarity in installations and a significant amount of service history is available for review, this determination can be an engineering judgment.

(iii) Hazards that have been identified and found to result from probable failures are not acceptable in multiengine airplanes. In these situations, a design change may be required to remove the hazard or to reduce the probability of failure, such as increasing redundancy, substitution of more reliable equipment, annunciation, etc.

(iv) If it has been determined that a probable failure or malfunction could result in a hazard to a single-engine airplane, that hazard should be minimized. To minimize is to reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. The least practical amount is that point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction. Additional efforts would not result in any significant improvements of safety and would inappropriately add to the cost of the

product without a commensurate benefit. This determination should come from an experienced engineering judgment based on the criticality of the hazard and the intended kinds of operation.

8. APPLICATION OF § 23.1309(a)(4), AS ADOPTED BY AMENDMENT 23-49.

a. For those commuter airplanes that include the certification basis of Amendments 23-34, 23-41, or 23-49, § 23.1309(a)(4) requires all applicable systems and installations to be designed to safeguard against hazards to the airplane in the event of their failure.

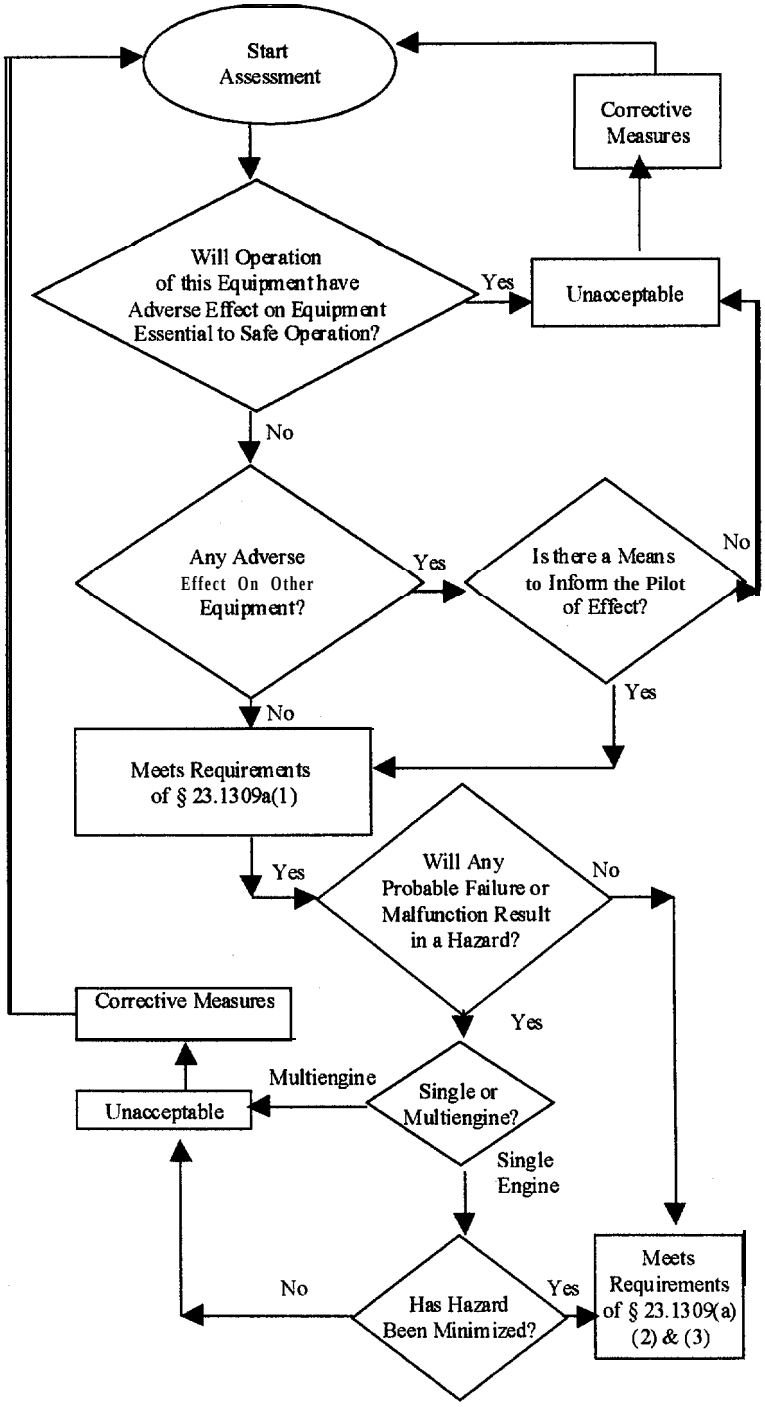
b. Design features should be taken into account to safeguard against hazards either by ensuring that the Failure Condition will not occur or by having redundancy or annunciation with the associated flight crew's corrective action. The reliability should be such that independent failures of the redundant systems are not probable during the same flight. If a redundant system is required, a probable failure in one system should not adversely affect the other system's operation. No probable failure should result in a safe indication of an unsafe condition so that the system would be used. When the unsafe condition is annunciated or detected, the Airplane Flight Manual (AFM) should have clear and precise corrective procedures for handling the failure without an excessive increase in workload.

c. Service history for similar installations may be utilized to meet part or all of this requirement if a system or installation has significant and favorable service history in environments similar to the airplane. The claim of similarity should be based on equipment type, function, design and installation similarities, and other relevant attributes.

9. APPLICATION OF § 23.1309(b), AS ADOPTED BY AMENDMENTS 23-41 AND 23-49.

a. If the certification basis is Amendment 23-41 or later, the requirements of § 23.1309(b) are applicable. The installed systems should be evaluated by performing a safety assessment. The depth and scope of the safety assessment depends on the types of functions performed by the systems, the severity of the Failure Conditions, and whether the system is complex. For instance, the safety assessment for a slightly modified single-engine airplane with simple systems might consist only of an FHA with a design and installation appraisal. This FHA will be much less extensive than the FHA for a commuter category or a multiple turbine-engine airplane with more complex systems. The types of analyses selected by an applicant and approved by the certification authority should be based on factors such as the system architecture, complexity, particular design, etc. This is described in more detail in Item 9.d.

FIGURE 1. METHOD TO COMPLIANCE DIAGRAM OF § 23.1309(a)



b. The safety objective is to ensure an acceptable safety level for equipment and systems installed on the airplane. A logical and acceptable inverse relationship should exist between the Average Probability Per Flight Hour and the severity of Failure Conditions effects (as shown in Figure 2). This figure defines the appropriate airplane systems probability standards for four certification classes of airplanes designed to 14 CFR Part 23 standards. The relationship between probability and severity of Failure Condition Effects is as follows:

- Failure Conditions with No Safety Effect have no probability requirement,
- Minor Failure Conditions may be Probable.
- Major Failure Conditions must be no more frequent than Remote.
- Hazardous Failure Conditions must be no more frequent than Extremely Remote.
- Catastrophic Failure Conditions must be Extremely Improbable.

(1) The four certification classes of airplanes in Figure 2 are as follows: Class I (Typically SRE under 6,000 pounds (#)), Class II (Typically MRE and STE under 6,000 pounds), Class III (Typically SRE, STE, MRE, and MTE equal or over 6,000 pounds), and Class IV (Typically Commuter Category). The acronyms for these airplanes in the four classes of Part 23 airplanes are Single Reciprocating Engine (SRE), Multiple Reciprocating Engine (MRE), Single Turbine Engine (STE), and Multiple Turbine Engine (MTE).

(2) Numerical values are assigned for use in those cases where the impact of system failures, is examined by quantitative methods of analysis. Also, the related new Software Development Assurance Levels for the various Failure Conditions are part of the matrix. The new probability standards are based on historical accident data, systems analyses, and engineering judgment for each class of airplane. For software, the requirements for complying with each Software Development Assurance Level are specified in RTCA DO- 178B.

(3) In assessing the acceptability of a design, the FAA recognized the need to establish rational probability values. Historically, failures in GA airplanes that might result in Catastrophic Failure Conditions are predominately associated with the primary flight instruments in Instrument Meteorological Conditions (IMC). Historical evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is approximately one per ten thousand hours of flight for single-engine airplanes under 6,000 pounds. Furthermore, from accident data bases, it appears that about 10 percent of the total were attributed to Failure Conditions caused by the airplane's systems. It is reasonable to expect that the probability of a fatal accident from all such Failure Conditions would not be greater than one per one hundred thousand flight hours or 1×10^{-5} per flight hour for a newly designed airplane. It is also assumed, arbitrarily, that there are about ten potential Failure Conditions in an airplane that could be catastrophic. The allowable target Average Probability Per Flight Hour of 1×10^{-5} was thus apportioned equally among these Failure Conditions, which resulted in an allocation of not greater than 1×10^{-6} to each. The upper limit for the Average Probability per Flight Hour for Catastrophic Failure Conditions would be 1×10^{-6}, which establishes an approximate probability value for the term "Extremely Improbable." Failure

FIGURE 2. RELATIONSHIP AMONG AIRPLANE CLASSES, PROBABILITIES, SEVERITY OF FAILURE CONDITIONS, AND SOFTWARE DEVELOPMENT ASSURANCE LEVELS

Classification of Failure Conditions	**No Safety Effect**	**<----Minor------>**	**+-Major---s**	**+-Hazardous-->**	**< Catastrophic>**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	**Allowable Quantitative Probabilities and Software (SW) Development Assurance Levels (Note 2)**				
Class I (Typically SRE under 6,000#)	No Probability or SW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 & 5 P=C, S=D P=D, S=D(Note 6)	$<10^{-5}$ Notes 4 & 5 P=C, S=D P=D, S=D(Note 6)	$<10^{-6}$ Note 3 P=C, s=c
Class II (Typically MRE or STE under 6000#)	No Probability or SW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 & 5 P=C, S=D P=D, S=D(Note 6)	$<10^{-6}$ Notes 4 & 5 P=C, s=c P=D, S=D(Note 6)	$<10^{-7}$ Note 3 P=C, s=c
Class III (Typically SRE, STE, MRE, & MTE equal or over 6000#)	No Probability or SW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 & 5 P=C, S=D	$<10^{-7}$ Notes 4 & 5 P=C, s=c	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically commuter Category)	No Probability or SW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 & 5 P=C, S=D	$<10^{-7}$ Notes 4 & 5 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: A numerical probability range is provided here as a reference. The applicant is usually not required to perform a quantitative analysis for Minor and Major Failure Conditions. See Figure 3.

Note 2: The alphabets denote the typical Software (SW) Development Assurance Levels as described in ARP 4754 for Primary System (P) and Secondary System (S). For example, SW Development Assurance Level A on Primary System is noted by P=A.

Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.

Note 4: At airplane function level, no single failure will result in the loss of a function that causes a Hazardous Failure Condition.

Note 5: Secondary System (S) may not be required to meet probability goals. If installed, S must meet stated criteria.

Note 6: A reduction of Software Development Assurance Levels applies only for Navigation, Communication, and Surveillance Systems if an altitude encoding altimeter transponder is installed. This option does not apply to CAT II/III operations.

Conditions having less severe effects could be relatively more likely to occur. Similarly, airplanes over 6,000 pounds have a lower fatal accident rate; therefore, they have a lower probability value for Catastrophic Failure Conditions.

c. Acceptable criteria for Software Development Assurance Levels of Part 23 airplanes are shown in Figure 2. Note 6 allows an additional reduction of Software Development Assurance Levels for Navigation, Communication, and Surveillance Systems if an altitude encoding altimeter transponder is installed. This option does not apply to CAT II/III operations. Software Development Assurance Levels in Figure 2, under Note 6, have been determined if an altitude encoding altimeter transponder is installed so that failure of navigation and communication systems used for IFR operations do not affect other airplanes. If the transponder is based on software, the software should be developed to at least Level C. If this option is used, the AFM must include a limitation such as, "A transponder with a valid altitude reporting mode must be operating for IFR operations unless otherwise instructed by ATC." Proper separation is provided by the Air Traffic Control (ATC) surveillance system and Traffic Collision Avoidance System (TCAS) equipped airplanes in IFR operations in the NAS or other equivalent airspace systems.

(1) The criteria shown in Figure 2 directly reflect the historical accident and equipment probability of failure data in the Civil Air Regulations (CAR) 3 and 14 CFR Part 23 airplane fleet. Characteristics of the airplane, such as stall speed, handling characteristics, cruise altitude, ease of recognizing system failures, recognition of entry into stall, pilot workload, and other factors (which include pilot training and experience) affect the ability of the pilot to safely handle various types of system failures in small airplanes. The criteria considered over all airplanes' Failure Conditions is based on service experience, operational exposure rates, and total airplane system reliability. The values for individual system probability of failure could be higher than probability values shown in Figure 2 for specific Failure Conditions since it considers the installed airplane systems, events, and factors.

(2) These classes were defined based on the way accident and safety statistics are currently collected. Generally, the classes deal with airplanes of historically equivalent levels of system complexity, type of use, system reliability, and historical divisions of airplanes according to these characteristics. However, these classes could change because of new technologies and the placement of a specific airplane in a class must be done in reference to all the airplane's missions and performance characteristics. The applicant should have the cognizant certification authority concurrence on the applicable airplane class early in the program. When unusual situations develop, consult the Small Airplane Directorate to obtain specific policy guidance or approval.

(3) For example, turbine-engine airplanes traditionally have been subject to more stringent requirements than a single-engine turbine airplane, with the fuel consumption of a reciprocating engine, which permits a wider stall-cruise speed ratio than traditional turbine-engine airplanes. Such an airplane with a stall speed under 61 knots with simple systems, and with otherwise similar characteristics to a traditional single-engine reciprocating airplane (except for a higher cruise speed and a more reliable engine that is simpler to operate), can be treated as a Class I airplane under this analysis. Conversely, if a single-engine reciprocating airplane has the performance, mission capability, and system complexity of a higher class (such as cabin pressurization, high cruise

altitude, and extended range), then that type of airplane design may align itself with the safety requirements of a higher class (for example, Class II airplane). These determinations should be made during the development of the certification basis.

(4) This AC uses terminology similar to AC 25.1309-l A. However, the specific means of compliance for § 25.1309 of Part 25 are defined differently due to the higher level of safety required for transport category airplanes.

d. ***Safety Assessments:*** The applicant is responsible for identifying and classifying each Failure Condition and for choosing the methods for safety assessment. The applicant should then obtain early concurrence of the cognizant certificating authority on the identification of Failure Conditions, their classifications, and the choice of an acceptable means of compliance. Figure 3 provides an overview of the information flow to conduct a safety assessment. This figure is a guide and it does not include ail information provided in this AC or the documents referenced in Item 3 of this AC.

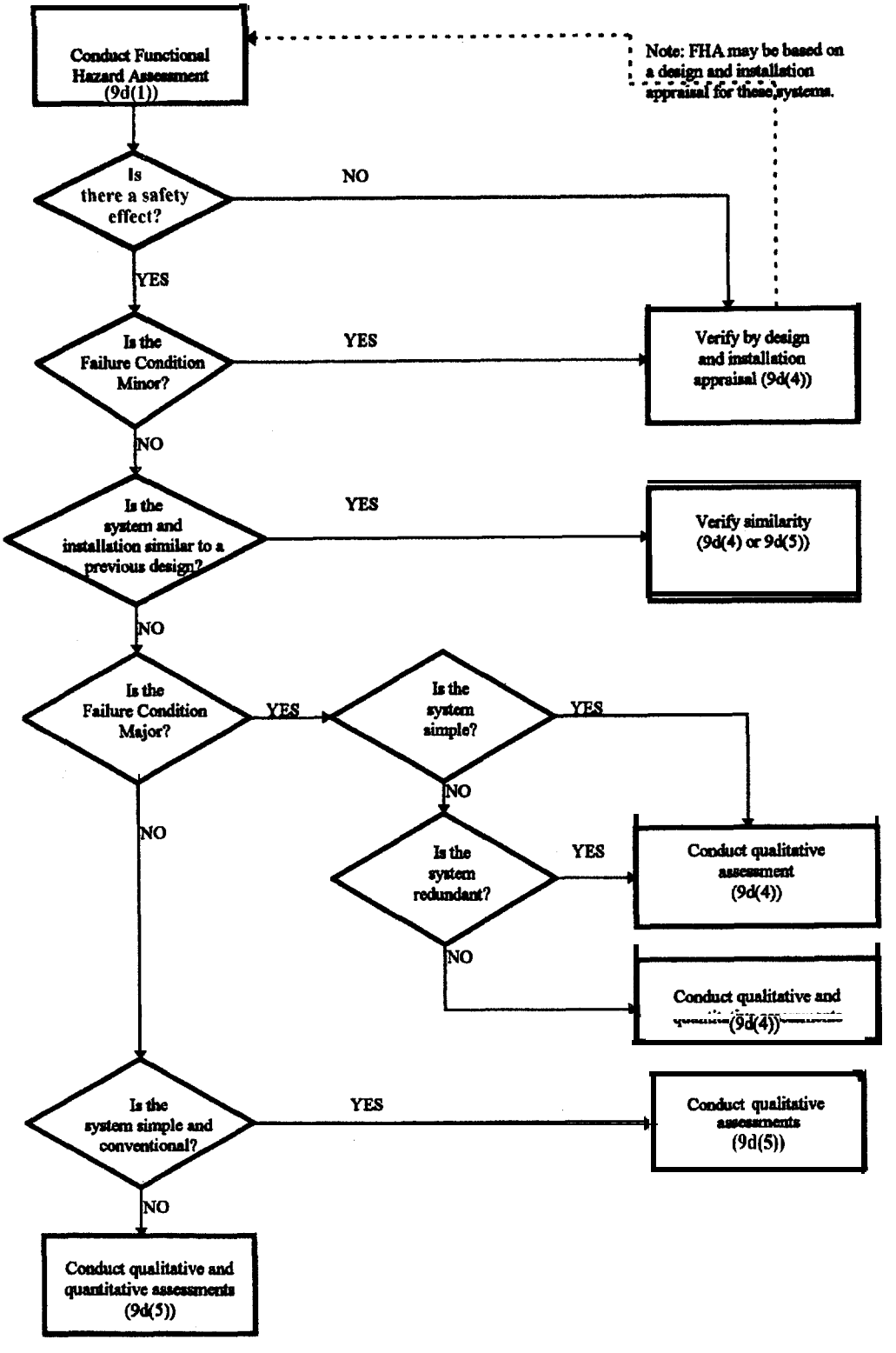
(1) Functional Hazard Assessment (FHA).

(i) Before an applicant proceeds with a detailed safety assessment, an FHA of the airplane and system functions to determine the need for and the scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgment, or service experience and a top-down deductive qualitative examination of each function. An FHA is a systematic, comprehensive examination of airplane and system functions to identify potential No Safety Effect, Minor, Major, Hazardous, and Catastrophic Failure Conditions that may arise, not only as a result of malfunctions or failure to function but also as a result of normal responses to unusual or abnormal external factors. The FHA concerns the operational vulnerabilities of systems rather than a detailed analysis of the actual implementation.

(ii) Each system function should be examined regarding the other functions performed by the system because the loss or malfunction of all functions performed by the system may result in a more severe failure condition than the loss of a single function. In addition, each system function should be examined regarding functions performed by other airplane systems because the loss or malfunction of different but related functions, provided by separate systems, may affect the severity of Failure Conditions postulated for a particular system.

(iii) The FHA is an engineering tool that should be performed early in the design and updated as necessary. It is used to define the high-level airplane or system safety objectives that must be considered in the proposed system architectures. Also, it should be used to assist in determining the development assurance levels for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An FHA requires experienced engineering judgment and early coordination between the applicant and the certification authority.

FIGURE 3. DEPTH OF ANALYSIS FLOW CHART



(iv) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to FHA may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interrelationships are relatively simple, it may be feasible to conduct separate FHA's for each system providing any interface aspects are properly considered and are easily understood. However, a top down approach, from an airplane level perspective, should be taken in planning and conducting FHA where system and function interrelationships are more complex.

(v) After each Failure Condition is classified, refer to Figure 2 to identify the Failure Condition probability and Software Development Assurance Levels. For example, the probability requirement for a Hazardous Failure Condition for a Class I airplane should be less than 1×10^{-5}. In addition, the Primary System should have a Software Development Assurance Level of C and, if required, the Secondary System should have a Software Development Assurance Level of D. However, if the airplane is equipped with an altitude encoding altimeter transponder for navigation, communication, and surveillance systems, the Primary System should have a Software Development Assurance Level of D and, if required, the Secondary System should have a Software Development Assurance Level of D.

(vi) The classification of Failure Conditions does not depend on whether a system or function is required by any specific regulation. Some systems required by specific regulations, such as transponders, position lights, and public address systems, may have the potential for only Minor Failure Conditions, Conversely, other systems not required by any specific regulation, such as flight management systems and automatic landing systems, may have the potential for Major, Hazardous, or Catastrophic Failure Conditions.

(vii) The classification of Failure Conditions should consider all relevant factors. Examples of factors include the nature of the failure modes, which includes common mode faults, system degradation resulting from failures, flight crew actions, flight crew workload, performance degradation, reduced operational capability, effects on airframe, etc. It is particularly important to consider factors that would alleviate or intensify the severity of a Failure Condition. An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by a Failure Condition. Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a Failure Condition, such as weather or other adverse operational or environmental conditions. The ability of a system to inform the pilot of potential or real Failure Conditions so that timely corrective action can be taken to reduce the effects of the combination of events is desirable. This approach may reduce the severity of the Failure Condition.

(A) Because of the large number of combinations of failures, various mitigating factors, airplane characteristic effects, and similar factors, a specific FHA and the related safety assessments may be significantly different for each airplane type and configuration evaluated. These factors preclude providing a concrete example of an FHA that applies across the board to every installation. However, general examples may be provided that illustrate the concepts involved in an FHA. It is critical to understand that significant engineering judgment and 'common sense are necessary to provide a practical and acceptable evaluation of the airplane and its systems. Appendix A provides a table that illustrates the criteria that may be applied to a system FHA

derived from the results of an aircraft FHA. Appendix A functional allocation examples CANNOT be applied indiscriminately to a particular airplane installation.

(B) Appendix A provides a partial FHA for Part 23 IFR Class I airplanes with typical **functions** and, in general, the related Failure Conditions. This table is provided primarily for use to reduce the regulatory burden on applicants who are not familiar with the various methods and procedures generally used in industry to conduct safety assessments. It is intended to be a guide and not a certification checklist, since it does not include all the information necessary for an FHA for a specific airplane with its various functions and its intended use. The functions are listed in the partial FHA as a guide for the classification of failure conditions when the functions are installed. The list of functions is not intended to suggest that the functions are required for the Class I airplanes. Even if there is guidance information in Appendix A, the applicable regulations provide the requirements of the functions for installations.

(1) The applicant should use Appendix A and certification authority as a point of departure for the assessment of the specific system or airplane in question. It can be used to arrive at the appropriate Failure Conditions for this specific system by similarity to or by interpolating between the example systems. It does not, by itself, necessarily provide an answer for an applicant's system unless that system is exactly as described. Its sole purpose is to assist applicants by illustrating typical functions and the related Failure Conditions. This appendix addresses general applicability, which is a value for determining Software Development Assurance Levels, and it should not be utilized to replace any specific guidance intended for individual types of equipment, systems, and installations. The FHA results are airplane characteristic and system architecture dependent. The examples in this appendix are based on the traditional airplane and traditional architectures. Because §23.1309 is a regulation of general requirements, it should not be used to supersede any specific requirements of Part 23.

(2) In addition to the general technical guidance provided in Appendix A, Appendix B provides a sample of one suggested format for documenting the results of an FHA. This format illustrates how factors other than those directly illustrated in Appendix A are pertinent. It also illustrates that Failure Conditions are not limited to only the three general types shown in Appendix A. The actual data shown in Appendix B is only used to illustrate the typical approach and should not be viewed as technically representative of any particular airplane. A complete FHA could be comprised of the layout shown in Appendix B by utilizing pertinent technical considerations identified in Appendix A, which are modified and expanded to reflect the specific proposed airplane design under consideration.

(C) Part 23 airplanes cover a wide range of airplane sizes and capabilities. These airplanes range from single-engine, single-seat, low-performance airplanes to complex multiengine, high-speed;high-performance airplanes. At the bottom end of these Part 23 airplane types, there are several compensating characteristics that mitigate many of the effects of a failure. Docile handling characteristics, low stall speeds, spin resistant designs, lower probability of operation in extreme weather conditions, and the inherent design philosophies used to design single-engine airplanes are specific examples of characteristics that may be considered in an FHA for systems installed in this class of airplane. Usually, support from ATC is not considered as a mitigating factor.

(2) Failure Conditions With No Safety Effect. An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these Failure Conditions. In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation. If the applicant chooses not to do the FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

(3) Analysis of Minor Failure Conditions. An analysis should consider the effects of system failures on other systems or their functions. An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these Failure Conditions. In general, common design practice provides physical and functional isolation from components that are essential to safe operation. If the applicant chooses not to do an FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

(4) Analysis of Major Failure Conditions. An assessment based on engineering judgment is a qualitative assessment, as are several of the methods described below:

(i) If the system is similar in its relevant attributes to those used in other airplanes and if the effects of failure would be the same, then a design and installation appraisal and satisfactory service history of either the equipment being analyzed or of a similar design is usually acceptable for showing compliance. It is the applicant's responsibility to provide accepted/approved data that supports any claims of similarity to a previous installation.

(ii) For systems that are not complex, where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment that shows that the Major Failure Conditions of the system as installed are consistent with the FHA (for example, redundant systems).

(iii) To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional FMEA supported by failure rate data and fault detection coverage analysis.

(iv) An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems, where functional redundancy is required, a qualitative FMEA and FTA may be necessary to determine that redundancy actually exists (for example, no single failure affects all functional channels).

(5) Analysis of Hazardous and Catastrophic Failure Conditions. For these failure conditions, a thorough safety assessment is necessary. The assessment usually consists of an appropriate combination of qualitative and quantitative analyses. Except as specified in Item 9.d.(5)(i) below, a detailed safety analysis will be necessary for each Hazardous and Catastrophic Failure Condition identified by an FHA. The analysis will usually be a combination of qualitative and quantitative assessments of the design,

(i) For simple and conventional installations (that is, low complexity and similarity in relevant attributes), it may be possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote or Extremely Improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for the assessment will be the degree of redundancy, the established independence and isolation of the channels, and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many airplanes may be sufficient when a close similarity is established regarding both the system design and operating conditions.

(ii) For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may also be possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote or Extremely Improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. A high degree of similarity in both design and application is required.

(iii) No Catastrophic Failure Condition (Note 3 in Figure 2) should result from the failure of a single component, part, or element of a system. Also, no single failure should result in the loss of a function that causes a Hazardous Failure Condition (Note 4 in Figure 2). In other words, it is acceptable to have a single failure for malfunction for a Hazardous Failure Condition if the probability values are met. Therefore, no single failure will result in any Catastrophic Failure Conditions or loss of a function for Hazardous Failure Condition. However, in unusual cases, experienced engineering judgment may enable an assessment that such a failure mode is not a practical possibility. The logic and rationale used in the assessment should be so straight forward and obvious that the failure mode simply would not occur unless it is associated with an unrelated Failure Condition that would, in itself, be Catastrophic.

(6) Assessment Methods. Methods for qualitatively and quantitatively assessing the causes, severity, and likelihood of potential Failure Conditions are available to support experienced engineering and operational judgment. Some of these methods are structured. The various types of analyses are based on either inductive or deductive approaches. The applicant should select analyses to validate the safety of a particular design based on factors such as the system architecture, complexity, criticality of the function, etc. ARP 4761 has more details of the various methods. Descriptions of typical types of analyses that might be used are provided below.

(i) ***Design Appraisal:*** A qualitative appraisal of the integrity and safety of the system design, such as the effective use of design techniques to verify that failures of a system do not adversely affect other systems. An effective appraisal requires experienced judgment.

(ii) ***Installation Appraisal:*** A qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications are made after entry into service.

(iii) ***Failure Modes and Effects Analysis (FMEA):*** A structured, inductive, bottom-up analysis that is used to evaluate the effects on the system and the airplane of each possible element or component failure. When properly formatted, it should aid in identifying latent failures

and the possible causes of each failure mode. ARP 4761 provides methodology and detailed guidelines that may be used to perform this type of analysis. An FMEA could be a piece-part FMEA or a functional FMEA. For modern microcircuit-based Line Replaceable Units (LRU) and systems, an exhaustive piece-part FMEA is not practically feasible with the present state of the art. In that context, an FMEA may be more functional than piece-part oriented. A functional-oriented FMEA can lead to uncertainties in the qualitative and quantitative aspects, which can be compensated for by more conservative assessments, such as the following:

(A) Assuming all failure modes result in Failure Conditions of interest,

(B) Carefully choosing system architecture, and

(C) Using lessons learned from similar technology.

(iv) ***Fault Tree Analysis (FTA):*** A structured, deductive, top-down analysis that is used to identify the conditions, failures, and events that would cause each defined Failure Condition. These are graphical methods of identifying the logical relationship between each particular Failure Condition and the primary element or component failures, other events, or combinations thereof that can cause it. After the fault tree is developed starting at the top and continuing on down to the most primary event at the bottom, an FMEA is usually used as the source document to verify the primary failures or other events.

(v) Common Cause Analysis: The acceptance of adequate probability of Failure Conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense, and specific studies are necessary to ensure that independence can either be assured or deemed acceptable. The "Common Cause Analysis" is divided into three areas of study:

(A) ***Zonal Safety Analysis:*** This analysis has the objective of ensuring that the equipment installations within each zone of the airplane are at an adequate safety standard regarding design and installation standards, interference between systems, and maintenance errors.

(B) ***Particular Risk Analysis:*** Particular risks are defined as those events or influences outside the systems concerned (for example, fire, leaking fluids, bird strike, tire burst, High Intensity Radiated Fields (HIRF) exposure, lightning, uncontained failure of high energy rotating machines, etc.). Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects, or influences, that may violate independence.

(C) Common Mode Analysis: This analysis is performed to confirm the assumed independence of the events that were considered in combination for a given Failure Condition. The effects of specification, design, implementation, installation, maintenance errors, manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered.

(7) Assessment Of Failure Condition Probabilities And Analysis Considerations. An assessment of the probability of a Failure Condition may be either qualitative or quantitative. An

analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the type of functions performed by the system, the severity of Failure Conditions, and whether the system is complex. A quantitative analysis is intended to supplement, but not replace, qualitative methods based on engineering and operational judgment. A quantitative analysis is often used for Catastrophic or Hazardous Failure Conditions of systems that are complex, that have insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems.

(i) A probability analysis may be either an FMEA or an FTA, which also includes numerical probability information. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analyses.

(ii) The probabilities of primary failures can be determined from failure rate data and exposure times using failure rates derived from either service experience on identical or similar items or from acceptable industry standards. Conventional mathematics of probability can then be used to calculate the estimated probability of each Failure Condition as a function of the estimated probabilities of the various identified contributory failures or other events.

(A) When calculating the estimated probability of each Failure Condition, a margin may be necessary to account for uncertainty. A margin is not normally required for an analysis that is based on proven data or from operational experience and tests. Where data has limited background for substantiation, a margin may be required depending on the available justification.

(B) The applicant should obtain early concurrence of the cognizant certification authority of an acceptable probability for each Major, Hazardous, and Catastrophic Failure Condition. Unless acceptable probability criteria are provided elsewhere, such as in other AC's, acceptable probabilities for Failure Conditions should be derived.

(C) The details on how to calculate the "Average Probability Per Flight Hour" for a Failure Condition are given in Appendix C of this AC. The "Average Probability Per Flight Hour" is the probability of occurrence, normalized by the flight time of a Failure Condition during a single flight. If the probability of a subject Failure Condition occurring during a typical flight of mean duration for the airplane type, divided by the flight's mean duration in hours, is likely to be significantly different from the predicted average rate of occurrence of that Failure Condition during the entire operational life of all airplanes of that type, then a risk model that better reflects the Failure Condition should be used. The single flight is analyzed to be representative of an average over all possible flights of the fleet of airplanes to be certified. The calculation of the "Average Probability Per Flight Hour" for a Failure Condition should consider the following:

(1) The average flight duration and the average flight profile for the airplane type to be certified. A common assumption for 14 CFR Part 23 airplanes is that the average flight duration is 1 hour,

(2) All combinations of failures and events that contribute to the Failure Condition,

(3) The conditional probability if a sequence of events is necessary to produce the Failure Condition,

(4) The relevant "at risk" time if an event is only relevant during certain flight phases, and

(5) The average exposure time if the failure can persist for multiple flights.

10. OPERATIONAL AND MAINTENANCE CONSIDERATIONS.

a. ***Flight Crew and Maintenance Tasks:*** These tasks, which are related to compliance, should be appropriate and reasonable. Quantitative assessments of the probabilities of flight crew and maintenance errors are not considered feasible. Reasonable tasks are those for which full credit can be taken because the flight crew or ground crew can realistically be anticipated to perform them correctly when they are required or scheduled. For the purposes of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and found to be reasonable. In addition, based on experienced engineering and operational judgment, the discovery of obvious failures during normal operation and maintenance of the airplane may be considered, even though such failures are not the primary purpose of focus of the operational or maintenance actions.

b. ***Flight Crew Action:*** When assessing the ability of the flight crew to cope with a Failure Condition, the information provided to the crew and the complexity of the required action should be considered.

(1) If the evaluation indicates that a potential Failure Condition can be alleviated or overcome in a timely manner without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, correct crew action may be assumed in both qualitative and quantitative assessments.

(2) Annunciation that requires flight crew actions should be evaluated to determine if the required actions can be accomplished in a timely manner without exceptional pilot skills. If the evaluation indicates that a potential Failure Condition can be alleviated or overcome during the time available without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, credit may be taken for correct and appropriate corrective action for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance if overall flight crew workload during the time available is not excessive and if the tasks do not require exceptional pilot skill or strength.

(3) Unless flight crew actions are accepted as normal airmanship, the appropriate procedures should be included in the FAA approved AFM or in the AFM revision or supplement. The AFM should include procedures for operation of complex systems such as integrated flight guidance and control systems. These procedures should include proper pilot response to cockpit

indications, diagnosis of system failures, discussion of possible pilot-induced flight control system problems, and use of the system in a safe manner.

c. Maintenance Actions: Credit may be taken for correct accomplishment of maintenance tasks in both qualitative and quantitative assessments if the tasks are evaluated and found to be reasonable. Required maintenance tasks, which mitigate hazards, should be provided for use in the FAA approved maintenance programs. Annunciated failures will be corrected before the next flight or a maximum time period will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. A scheduled maintenance task may detect latent failures. If this approach is taken, and the Failure Condition is Hazardous or Catastrophic, then a maintenance task should be established. Some Latent Failures can be assumed to be identified based upon a return to service test on the equipment following its removal and repair (component Mean Time Between Failures (MTBF) should be the basis for the check interval time).

11. ELECTROMAGNETIC PROTECTION FOR ELECTRICAL/ELECTRONIC SYSTEMS.

a. Background: Current trends indicate increasing reliance on electrical/electronic systems for safe operations. For systems that perform flight, propulsion, navigation, and instrumentation functions, electromagnetic effects should be considered.

b. High Intensity Radiated Fields (HIRF):

(1) The words "radio frequency energy" in § 23.1309(e) are not intended to include HIRF; therefore, special conditions must be issued until the HIRF requirements are incorporated into Part 23 in a final rule. These special conditions are applicable for systems that perform functions whose failure to provide that function correctly could lead to a Catastrophic Failure Condition. A notice provides guidance material relevant to certification of airplanes for HIRF. Airplanes are exposed to the HIRF environment, which results from high-power radio frequency transmitters such as radio and television broadcast stations, radar, and satellite ground-earth stations. This notice provides a standard and uniform set of requirements for an airplane certification until a final rule can be issued. Airplane electrical and electronic systems, or equipment addressed by this notice, may include new designs, significant modifications of existing designs, applications of existing systems, or equipment that has not been previously certified for HIRF.

(2) The FAA/Joint Aviation Authorities (JAA) Electromagnetic Effects Harmonization Working Group of the Aviation Rulemaking Advisory Committee (ARAC) developed a Notice of Proposed Rulemaking (NPRM). This NPRM received the participation of international airworthiness authorities, industry, and industry groups in developing the proposed international standards. The NPRM is now in the rulemaking process. Special conditions will be necessary until this rule is issued.

c. Lightning Protection:

(1) Section 23.1309(e) contains the regulatory requirements for the protection of airplane electrical/electronic systems against the indirect effects of lightning. These requirements are applicable for electrical/electronic functions whose Failure Conditions are classified as Catastrophic, Hazardous, or Major. For guidance, AC 20-136 and Section 22 of RTCA/DO-160D, or subsequent revisions, provide acceptable methods and procedures for determining compliance with the indirect effects of lightning requirements. AC 20-136 provides guidance to verify the protection of systems installed in an aircraft. Section 22 of RTCA/DO-160D provides methods to qualify equipment prior to installation in an airplane.

(2) For those airplanes intended for operation under IFR, a more detailed assessment will need to be made concerning the vulnerability to lightning related hazards. The need for lightning protection for systems on airplanes limited to VFR operations is determined on a case-by-case basis. The depth of the verification should be commensurate with the degree of hazard. Airplanes that employ proven conventional construction and systems (that is, all-aluminum airplanes with gyroflight instruments, magneto-type engine ignition systems, mechanical fuel systems, etc.) have demonstrated excellent inherent lightning protection qualities over many millions of flight hours. Similar designs may only need a qualitative engineering assessment that all hazards have been reasonably minimized. DOT/FAA/CT-89/22 may be used as a guide to make this assessment. Other designs (that is, all composite construction, or installation of electronic flight instrument displays, electronic ignition, or electronic fuel systems, etc.) are generally more susceptible to lightning threats; therefore, these designs will need further evaluation. The methods outlined in AC's 20-53A, 20-136, and 23-15, and RTCA DO-160D provide acceptable means of compliance with the requirements, as applicable.

(3) Functions performed by systems whose Failure Conditions are classified as Hazardous or Major would require protection to the extent that the function should recover in a timely manner after the airplane has been exposed to lightning. Testing and analysis are directed toward a component damage (that is, a damage tolerance test). Multiple stroke and multiple burst testing should not be required; therefore, the laboratory test procedures in RTCA/DO-160D are acceptable. Multiple stroke and multiple burst testing should not be required for systems that perform functions whose Failure Conditions are classified as Hazardous or Major if an analysis shows that the equipment is not susceptible to upset or that the equipment may be susceptible to upset but a reset capability exists that will recover the function in a timely manner. A specific category or level of testing as defined in RTCA/DO-160D is not being given, but a simple analysis method by experienced engineering judgment is normally sufficient to determine the appropriate testing level. Systems that have been previously approved may be approved by similarity provided there has been no unresolved in-service history of problems relating to lightning strikes to the aircraft.

(4) Functions whose Failure Conditions are classified as Catastrophic would require protection to the extent that the function should not be adversely affected when the airplane is exposed to lightning. These functions should continue to be provided during and after exposure to lightning. If the function is provided by multiple systems, then loss of a system or systems during exposure of the airplane to lightning should not result in the loss of the function. After the airplane

is exposed to lightning, each affected system that performs these functions should automatically recover normal operation, unless this conflicts with other operational or functional requirements of that system. Neither multiple stroke and multiple burst testing nor analysis should be required for damage assessment, but these can be the primary factors in a system functional upset.

(5) Appendix 3 of AC 20-136 defines total lightning environment, including the multiple stroke and multiple burst lightning environment to be used for test and analysis purposes in qualifying systems and equipment for lightning protection. AC 20-136 is proposed as a basis to use in demonstrating compliance with the lightning protection requirements, except for the multiple burst lightning environment that has been changed to agree with recommendations from the Society of Automotive Engineers (SAE) AE4L Committee, dated July 6, 1992. The multiple burst lightning environment that is defined in AC 20-136 has been changed from 24 bursts to 3 bursts and it is used mainly for test and analysis of system functional upset.

12. DEVELOPMENT ASSURANCE FOR AIRBORNE SYSTEM AND APPLICATIONS.

a. ***Background:*** AC 20-115B discusses how RTCA/DO-178B provides an acceptable means for showing that software complies with pertinent airworthiness requirements.

b. ***Acceptable Application of Software Development Assurance Levels:*** It is necessary to consider the possibility of requirement, design, and implementation errors in order to comply with the requirements of §23.1309(b). Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components by direct inspection and by other direct verification methods capable of completely characterizing the performance of the system. These direct techniques may still be appropriate for simple systems, which perform a limited number of functions and which are not highly integrated with other airplane systems.

(1) For more complex or integrated systems, exhaustive testing may either be impossible because all of the systems states cannot be determined or it may be impractical due to the number of tests that must be accomplished. For these types of systems, compliance may be shown by the use of Software Development Assurance Levels. The Software Development Assurance Levels should be determined by the severity of potential effects on the airplane in case of system malfunctions or loss of functions.

(2) Criteria for Software Development Assurance Levels of Part 23 airplanes are shown in Figure 2. The levels in Figure 2 are considered acceptable instead of the Software Development Assurance Levels defined in paragraph 2.2.2 in RTCA/DO-178B. Additional guidelines, which may be used for determining Software Development Assurance Levels, are described in ARP 4754 and RTCA/DO-178B. Because these documents were not developed simultaneously, there are differences in the guidelines and terminology.

(3) There is a significant difference in the guidance provided on the use of system architecture for determination of the appropriate Software Development Assurance Levels. The FAA recognizes that consideration of system. architecture for this purpose is appropriate. Where

apparent differences exist between these two documents on this subject, then the guidance contained in ARP 4754 should be used if additional credit for architecture is requested for Hazardous or Catastrophic Failure Conditions in commuter category airplanes.

(4) Equipment installed in Part 23 airplanes that performs functions addressed by TSO standards should meet applicable TSO standards, but the equipment is not required to have TSO authorization. Some TSO equipment specifies minimum Software Development Assurance Levels. Software for non-TSO equipment installed in Part 23 airplanes may use the Software Development Assurance Levels of Figure 2 in lieu of the levels specified in the TSO.

c. Acceptable Application of Hardware Development Assurance Levels: There are currently no agreed standards for hardware development assurance levels. The RTCA Special Committee (SC) 180 is developing more details on methods for substantiating hardware development assurance levels.

Michael Gallagher
Manager, Small Airplane Directorate
Aircraft Certification Service

AC 23.1309-1C -APPENDIX A. "PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of attitude information to control roll and pitch	Catastrophic	Major	Catastrophic	For electronic displays, dual independent attitude systems generally meet requirements for 14 CFR Part 23, § 23.1311 and for conventional mechanical or analog electromechanical systems, a single attitude display meets requirements to operate under Instrument Flight Rules (IFR) for Part 9 1. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. Partial panel techniques may be used in some cases where it has been historically shown to be acceptable. Credit (mitigation) may be given for automatic flight control systems if the system can maintain stable attitude independent of the primary attitude display.
Display of directional heading information	Major	Minor	Major	Assumes installation of a single stabilized heading system and only a non-stabilized magnetic compass to operate under Instrument Flight Rules (IFR) for Part 9 1. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. Navigation assumed to be operating.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A, *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of altitude information	Hazardous	Minor	Catastrophic	For electronic displays, dual independent altitude systems generally meet requirements for 14 CFR Part 23, $23.13 I 1 and for conventional mechanical or analog electromechanical systems, a single altitude display meets requirements to operate under Instrument Flight Rules (IFR) for Part 91. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. Existing single static systems that are heated have been historically acceptable based on similarity and may be used for programs that have certification basis prior to Amendment 23-42. If a single or dual air data computer is used, it must meet the requirements of this AC with respect to safety and Software Development Assurance.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of airspeed information	Major. May be Hazardous for higher performance airplanes.	Minor	Major. May be Hazardous for higher performance airplanes.	For electronic displays, dual independent airspeed systems generally meet requirements for 14 CFR Part 23, § 23.13 11 and for conventional mechanical or analog electromechanical systems, a single airspeed display meets requirements to operate under Instrument Flight Rules (IFR) for Part 9 1. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. Classification as Major, if overspeed and underspeed airspeed alerting is acceptable (alerting may be provided by inherent aerodynamic qualities or independent alerting system); otherwise, loss of function, malfunction, or misleading of information is Hazardous. Assumes no vertical speed indicator. Existing single pitot static systems that are heated have been historically acceptable based on similarity and may be used for programs that have certification basis prior to Amendment 23-42. If a single or dual air data computer is used, it must meet the requirements of this AC with respect to safety and Software Development Assurance Levels.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of rate-of-turn information	Minor	Minor	Minor	Rate-of-turn display is generally required to operate under instrument Flight Rules (IFR) for Part 91 unless a third attitude is installed. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. In Instrument Meteorological Conditions (IMC) misleading rate-of-turn information is consider to be Minor if there is a functional attitude display.
Display of slip-skid information	Minor	Minor	Minor	R
Display of time information	Minor	Minor	Minor	R
Display of navigation information	Major	Major. Minor, if two navigation systems are installed.	Major. May be Hazardous for precision approaches.	Two navigation systems are generally installed to support navigation, but two are not required for 14 CFR Part 91 operations. May use the combination of all data in pilot's eye scan. Dual Instrument Landing Systems (ILS) receivers below Category I limits are required with single antenna for Part 91 operations.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Communication	Minor. Total loss of navigation and communication is Hazardous	Minor	Major, if data link. Otherwise, Minor.	Future installations may use data link for primary functions and voice for secondary.
Display of radio altitude information	Minor	R	Minor	Not required for 14 CFR Part 91 operations, Category I ILS. Loss of function may affect other equipment that depends upon radio altimeter, such as GPWS, etc.
Display of vertical speed information	Minor	R	Minor	Not required for 14 CFR Part 91 operations.
Display of flight guidance commands (Category I operation)	Minor	R	Minor	Not required for 14 CFR Part 9 1 operations, Category I ILS. For Category II ILS, an autopilot or flight director is required.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Autopilot	Minor, with warning. Major, without warning.	R	Major, single axis and limited authority. Hazardous, multi-axis and limited authority. Catastrophic, if authority is unlimited.	Maximum inputs (hardovers) or (slowovers) to aircraft primary control surfaces should not exceed aircraft structural limits. Refer to AC 23.1329-2, "Automatic Pilot System Installation in Part 23 Airplanes."
Electrical-Electronic primary powered flight controls	Catastrophic. Hazardous for loss of one lateral axis.	Minor	Catastrophic	Assumes redundant electrical/electronic primary flight control systems with no manual reversion that provide independent control for each axis.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Stability augmentation	Variable	Minor	Variable	It needs to be evaluated on a case-by-case basis since it depends on aircraft stability and handling characteristics when installed and required to meet minimum performance and flight handling requirements.
Stick pusher	If loss is not annunciated, then Hazardous; .if failure indication is given, then Minor.	Minor	Catastrophic	The system is installed to protect against a Hazardous stall characteristic. Assumes dual systems to prevent single-failure modes. Stick pusher malfunction with or without warning can be Catastrophic depending on phase of flight and system attributes. Airplane response to stick pusher may be considered and pilot procedures may mitigate to a lower Failure Condition.
Stick shakers/stall warning	Minor	Minor	Major	Assumes that a warning system is in place to notify pilot that loss of system function has occurred (for example, stick force changes, buffeting, inherent aerodynamics features, etc.).

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-r C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Trim control	Minor	Minor	Major, if manual trim. Catastrophic or Hazardous for electrical.	Studies have shown trim runaways are not a significant problem if pilot takes quick corrective action. Major, for trim runaways if there is a trim-in-motion aural alert. Hazardous or Catastrophic, for trim runaways without a failure indication depending on trim authority.
Gear control	Major	Minor	Major	R
Brake control	Major, for airplanes ≥ 6,000#. Minor, for airplanes < 6,000#.	Major. Could be Minor, if thrust reversers are installed.	Major	Electronic anti-skid and brake systems can cause significant ground handling problems if they malfunction under adverse conditions due to asymmetrical loading. Light airplanes braking loss is not as significant and can be reviewed on a case-by-case basis.
Display of trim indications	Minor	Minor	Variable	Each airplane has to be reviewed on a case-by-case basis.
Display of gear indications	Minor	R	Minor	R

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of fuel level indication	Minor	Minor	Minor	Pilot is required to calculate fuel range and endurance during normal flight planning operations.
Display of power-plant indication tachometer	Minor	Minor	Minor	Assumes fixed pitch propeller and reciprocating engine; otherwise, a propeller governor will maintain the engine r.p.m. Turbofan and turbojet engines may need r.p.m. data for inflight restart capability. Refer to 14 CFR Part 23, § 23.13 11.
Display of power-plant Cylinder Head Temperature (CHT)	Minor	Minor	Minor	Assumes a CHT indicator is required. Refer to 14 CFR Part 23, $23.1305.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of power-plant indication coolant temperature	Minor	Minor	Minor	Rcferto 14 CFR Part 23, § 23.1305.
Display of powerplant indication oil pressure	Minor	Minor	Minor	Assumes oil temperature is used as a backup.
Display of powerplant indication oil temperature	Minor	Minor	Minor	Assumes oil pressure is used as a backup.
Display of powerplant indication manifold pressure	Minor	Minor	Minor	Assumes backup use of CIIT, Engine Gas Temperature (EGT), and possible fuel flow readings if installed.
Display of powerplant air inlet temperature	Minor	Minor	Minor	R

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of power-plant indication fuel pressure	Minor	Minor	Minor	R
Display of powerplant indication gas temperature for turbine engine	Minor	Minor	Major	Torque indication can be used as an emergency backup indicator to control the engine to a safe landing.
Display of powerplant indication fuel flow	Minor	Minor	Major	Manifold pressure and r.p.m. or torque indications can be used as an emergency backup to control power until a safe landing can be made.
Display of powerplant fire warning	Major	Major	Hazardous	Required for commuter category and Part 23 turbojet powered airplanes using special conditions. Part 23 airplanes usually have one fire warning system on board.
Display of powerplant indication thrust	Minor	Minor	Hazardous	System is not normally used in Part 23 airplanes. Torque, Engine Pressure Ratio (EPR), EGT, or Turbine Inlet Temperature (TIT), fuel flow, and r.p.m. are the parameters normally displayed.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-l C -APPENDIX A. *PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Display of powerplant thrust reverser position	No effect	No effect	Major	No certification credit is given for enhanced performance when a thrust reverser is installed.
Thrust reversal	Minor	Minor	Variable (inadvcrtcnt deployment)	No certification credit is given for enhanced performance when a thrust reverser is installed. No credit can be given for a warning.
Display of powerplant torque	Minor	Minor	Major	Misleading torque could affect takeoff performance.
Display of powerplant propeller blade angle	No safety effect	No safety effect	No safety effect	System is not normally used in Part 23 airplanes. Propeller governor would control r.p.m.
Visual warnings, cautions, and alerts	R	R	R	Failure Conditions depend on the criticality of systems being monitored and pilot action required.
Display of air temperature	Minor	R	Minor	

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX A. 'PARTIAL FUNCTIONAL HAZARD ASSESSMENT (FHA) TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	Loss of Primary Means of Providing Function	Misleading and/or Malfunction Without Warning	
Overspeed warning	Minor	Minor	Minor	Airspeed may be used as a backup to the overspeed warning for continued safe flight and landing.
Aural warnings	R	R	R	Aural alerts tend to be reserved for required flight crew's immediate corrective action. Failure Conditions depend on the criticality of the system.
Electrical system indication	Minor	Minor	Major	Depends on crew reference and analysis.
Vacuum/pressure indication	Minor	Minor	Major	Provides an indication that flight instruments are operating within power source limits.
Electrical power	Catastrophic, if primary flight instruments require electrical power.	Hazardous for IFR. Depends upon capability of secondary power system.	Installation dependent	Depends on electrical system loads and the criticality of the functions.

*Note: This table is intended to be a guide and not a certification checklist since it may not include all the information necessary for an FHA on Part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop an FHA. See Item 9d(1) and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

AC 23.1309-1C -APPENDIX B. *SAMPLE FUNCTIONAL HAZARD ASSESSMENT (FHA) FORMAT

Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to supporting Material	Verification
Display of attitude information to control roll and pitch	Annunciated loss of primary means (but not all) of attitude information used for control in roll and pitch.	All	Crew would not be able to use primary means of attitude information, and would have to resort to backup means. As long as it is clear that the primary means cannot be relied upon, then backup means would create an increase in crew workload, but doubtful anything more severe. Hypothetical cases where it is not clear as to the integrity of the information may come under the "Misleading attitude information" case below.	Major		Aircraft Fault tree
	Loss of all means of attitude information.	All	Assuming TFR conditions, the crew would unknowingly follow incorrect attitude information, and inadvertently exceed attitude limits, which could result in the loss of control of the aircraft.	Catastrophic		Aircraft fault tree

*Note: This sample FHA is intended to be a guide for format purposes only to illustrate what items should be considered when performing an FHA. Since other pertinent information regarding the type of airplane and its features is not provided, the technical content may not be appropriate for other airplanes. See Item 9(d)(l) and its associated subparagraphs for more complete guidance.

AC 23.1309-1C -APPENDIX B. *SAMPLE FUNCTIONAL HAZARD ASSESSMENT (FHA) FORMAT

Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to supportiug Material	Verification
Display of attitude information to control roll and pitch	Incorrect attitude information on some display, but not on all displays (not misleading in nature).	All	Generally, this condition would be the loss of one means of attitude information. For this condition, the crew would realize that this information was incorrect. If there is any chance this would not be clear, the scenario would have to be considered "Misleading attitude information" as described below.	Major		Aircraft fault tree
	Misleading attitude information: Note: if misleading data could be provided to the autopilot, that is handled under the autopilot failure conditions.	All	Assuming TFR conditions, the crew would unknowingly follow incorrect attitude information, and inadvertently exceed attitude limits which could result in the loss of control of the aircraft.	Catastrophic		Aircraft fault tree
(Next Function)	(First Related Failure Condition)					
	(Next Related Failure Condition, and so on)					

*Note: This sample FIIA is intended to be a guide for format purposes only to illustrate what items should be considered when performing an FHA. Since other pertinent information regarding the type of airplane and its features is not provided, the technical content may not be appropriate for other airplanes. See Item 9(d)(1) and its associated subparagraphs for more complete guidance.

APPENDIX C. CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR

The purpose of this material is to provide guidance for calculating the "Average Probability Per Flight Hour" for a Failure Condition so that it can be compared with the quantitative requirements of 14 CFR Part 23, $23.1309.

The process of calculating the "Average Probability Per Flight Hour" for a Failure Condition will be described as a four-step process and is based on the assumption that the life of an aircraft is a sequence of "Average Flights."

Step 1: Determination of the "Average Flight;"
Step 2: Calculation of the probability of a Failure Condition for a certain "Average Flight;"
Step 3 : Calculation of the "Average Probability Per Flight" of a Failure Condition; and
Step 4: Calculation of the "Average Probability Per Flight Hour" of a Failure Condition.

a. Determination of the "Average Flight: " The "Average Probability Per Flight Hour" is to be based on an "Average Flight. " The applicant should estimate the average flight duration and average flight profile for the fleet of aircraft to be certified. The average flight duration should be estimated based on the applicant's expectations and historical experience for similar types. The average flight duration should reflect the applicant's best estimate of the cumulative flight hours divided by the cumulative aircraft flights for the service life of the aircraft. The average flight profile should be based on the operating weight and performance expectations for the average aircraft when flying a flight of average duration in an International Civil Aviation Organization (ICAO) standard atmosphere. The duration of each flight phase (for example, takeoff, climb, cruise, descent, approach and landing) in the "Average Flight" should be based on the average flight profile. Average taxi times for departure and arrival at an average airport should be considered where appropriate and added to the average flight time to obtain "Average Flight--Block Time." The average flight duration and profile should be used as the basis for determining the "Average Probability Per Flight Hour" for quantitative safety assessment on compliance with the requirements of this AC.

b. ***Calculation of the Probability of a Failure Condition for a certain "Average Flight:"*** The probability of a Failure Condition occurring on an "Average Flight" should be determined by structured methods (see ARP 4761 for various methods) and should consider all elements (for example, combinations of failures and events) that contribute to a Failure Condition. If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce a Failure Condition. The probabilities of the basic events (component or part level failures) that contribute to the probability of a Failure Condition should consider the following:

(1) The individual part, component, and assembly failure rates utilized in calculating the "Average Probability Per Flight Hour" should be estimates of the mature constant failure rates

after infant mortality and prior to wear out, and should be based on all causes of failure (operational, environmental, etc.). Where available, service history of same or similar components in the same or in a similar environment should be used.

(2) If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant "at risk" time for the "Average Flight."

(3) If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation has to consider the relevant exposure times (for example, time intervals between maintenance checks/ inspections). In such cases, the probability of the Failure Condition increases with the number of flights during the latency period.

(4) If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the Failure Condition occurring on an "Average Flight." It is assumed that the "Average Flight" can be divided into n phases (phase 1, . . . , phase n). Let T_F the "Average Flight" duration, T_j the duration of phase j and t_j the transition point between T_j and T_{j+1}, j = 1, . . . , n . I.e.

$$T_F = \sum_{j=1}^{n} T_j \text{ and } t_j - t_{j-1} = T_j \; ; j = 1, \ldots, n$$

Let $\lambda_j(t)$ the failure rate function during phase j, i.e. for $t \in [t_{j-1}, t_j]$.

Remark: $\lambda_j(t)$ may be equal 0 for all $t \in [t_{j-1}, t_j]$ for a specific phase j.

Let P_{Flight} (Failure) the probability that the element fails during one certain flight (including non-flying time) and $P_{Phase\ j}$ (Failure) the probability that the element fails in phase j.

Two cases are possible:

(i) The element is checked operative at the beginning of a certain flight. Then

$$P_{Flight}\ (Failure) = \sum_{j=1}^{n} P_{Phase\ j}(Failure) = \sum_{j=1}^{n} P\left(Failure \middle| t \in \left[t_{j-1},\ t_j\right]\right)$$

$$= 1 - \prod_{i=1}^{n} \exp\left(- \int_{t_{i-1}}^{t_i} \lambda_i(x)\, dx \right)$$

(ii)The state of the item is unknown at the beginning of a certain flight. Then

$$P_{Flight}\ (Failure) = P_{prior}(Failure) + \left(1 - P_{prior}(Failure)\right) \cdot \left(1 - \prod_{i=1}^{n} \exp\left(- \int_{t_{i-1}}^{t_i} \lambda_i(x)\, dx \right) \right)$$

where P_{prior} (Failure) is the probability that the failure of the element has occurred prior to a certain flight.

(5) If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce a Failure Condition.

*c. **Calculation of the "Average Probability Per Flight" of a Failure Condition:*** The next step is to calculate the "Average Probability Per Flight" for a Failure Condition, that is, the probability of a Failure Condition for each flight (which might be different, although all flights are "Average Flights") during the relevant time (for example, the least common multiple of the exposure times or the aircraft life) have to be calculated, summed up, and divided by the number of flights during that period. The principles of calculating are described below and are in more detail in ARP 476 1.

$$P_{Average\ per\ Flight}\ (Failure\ Condition) = \frac{\sum_{k=1}^{N} P_{Flight\ k}\ (Failure\ Condition)}{N}$$

Note: N is the quantity of all flights during the relevant time, and $P_{Flight\ k}$ is the probability that a Failure Condition occurs in flight k.

Example: In the special case of a duplex system (one component failure latent, the other detected), this method results in an "Average Probability Per Flight," which equals the product of both failure rates multiplied by the

"Average Flight" duration T_F multiplied by one-half (50 percent) of the relevant exposure time.

d. ***Calculation of the "Average Probability Per Flight Hour" of a Failure Condition:*** Once the "Average Probability Per Flight" has been calculated, it should be normalized by dividing it by the "Average Flight" duration T_F in "Flight Hours" to obtain the "Average Probability Per Flight Hour." This quantitative value should be used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant for the Failure Condition being analyzed.

$$P_{\text{Average per FH}}(\text{Failure Condition}) = \frac{P_{\text{Average per Flight}}(\text{Failure Condition})}{T_F}$$

U.S. Department
of Transportation

**Federal Aviation
Administration**

800 Independence Ave., S.W.
Washington, DC. 20591

**FORWARDING AND ADDRESS
CORRECTION REQUESTED**

Official Business
Penalty for Private Use $300